

*MY PLEDGE-CYBER BULLYING  
STOPS WITH ME...IF I SEE  
SOMETHING I WILL SAY  
SOMETHING*



## What is Cyber Smarts?

Students helping students to stay safe while:

- Gaming
- Using Social Media
- Sending Texts and Emails
- Downloading from the web
- Shopping on the internet

## Why Cyber Smarts?

What you post on the web never goes away!  
Online predators troll the Web

Online shopping is not without risk

Cyber bullying has real world implications!

## CYBER SMARTS

PRESENTED BY:  
ELTON CARVALHO  
ALEX SANCHEZ  
TOLMAN HIGH SCHOOL  
PAWTUCKET, RI



Contact:  
Brian J. Pires  
National Security Specialist  
Law Enforcement Coordinator  
US Attorneys District of Rhode Island  
(401) 714-4284

## Cyber Smarts

*Cyber Smarts* is a preventive program designed for students by students.

*Cyber Smarts* is geared toward middle and high school students.

*Cyber Smarts* addresses contemporary risks teens may experience while online and when using social media.

### Internet Shopping

- **DANGERS OF BEING SCAMMED WHEN BUYING OR SELLING THINGS ONLINE**
  - When buying things online, be wary of unfamiliar links
  - Be wary of purchasing items from foreign countries
  - If you are selling something stay in a lane you're comfortable with don't try to use any money transferring programs or sites you are unfamiliar with
  - Don't give out your home address and be careful of sharing locations (manage your privacy settings turn off location/geotagging. Make sure pics are not geotagged)



### Unprotected Sites

Unprotected sites seek to steal your information, basically your identity, you should look out for:

- Be wary of sites that do not have an "s" (https)
- Look for unbelievable domain names for websites  
[www.freenikeshoes.com](http://www.freenikeshoes.com)
- Provide No contact info like a number and address
- Have grammar and spelling errors
- Check reviews!

Avoid being a victim...Remember

**DON'T** share device passwords with anyone you don't fully trust.

**DON'T** take pictures of yourself you wouldn't want the public/your parents to see.

**Think before you post!**

The more info you post about yourself, the more vulnerable you are.

### Phishing E-mails

Scammers try to lure you into a trap using emails that are very well crafted. They may appear to be from a friend or colleague.

If the language or request does not seem to be like something that friend or colleague would normally ask for **BEWARE!**

Scammers hope you will click on an attachment that will load malware onto your device or attempt to solicit personal information.

"Holiday season" -email appears to be from a legitimate company such as Amazon or eBay ref. "your recent purchase"

Beware of clicking any attachments it might release any malware particularly files with .exe

### What To Look Out For-Suspicious Emails...

Spelling Mistakes

Strange email address

Suspicious links...hover for cover and don't click!

Emails requesting personal information, asking for money and/or unusual requests

